Office of the
Comptroller of the Currency

April 14, 2025

Subject: OCC Information Security Incident

Dear CEO:

On April 8, 2025, the Office of the Comptroller of the Currency (OCC), in accordance with the Federal Information Security Modernization Act (FISMA), notified Congress that it identified a major incident resulting from a breach of the OCC's email system. The breach occurred when an unauthorized user accessed a number of OCC user accounts, including emails and attachments, via a service account with administrative-level privileges. The OCC immediately disabled the unauthorized account and is now determining what data has been accessed, including the extent to which highly sensitive information relating to the financial condition of federally regulated financial institutions was compromised. The OCC has also deployed enhancements and improvements to IT security to ensure a robust data security environment.

Background: On February 11, 2025, Microsoft Global Hunting Oversight and Strategic Triage (GHOST) notified the OCC that they observed unusual interactions between a service account in Microsoft's Azure office automation environment and OCC user mailboxes hosted by Microsoft. Authentications to this service account were tracked to a location associated with a commercial Virtual Private Network (VPN) service.

On February 12, the OCC confirmed the activity was unauthorized and immediately activated its incident response protocols. This included initiating an independent third-party forensics and incident assessment of the breach by Mandiant and reporting the incident to the Cybersecurity and Infrastructure Security Agency (CISA) as required per M-25-04. The OCC subsequently secured the services of CrowdStrike to conduct a similar investigation.

During its extensive internal review, the OCC learned that the unauthorized access involved sensitive information. On April 7, the OCC determined the incident qualified as a major incident under FISMA.

OCC Response: In response to the unauthorized activity, the OCC disabled the compromised service account and confirmed the unauthorized access had been terminated. The OCC also globally reset all credentials associated with its full Microsoft tenant to eliminate the possibility of further unauthorized access by this threat actor. At this time, the OCC has confirmed the universe of the compromised email mailboxes, dates of compromise, and messages and attachments accessed during the incident. Efforts to analyze the compromised email messages to determine their contents have been initiated and are ongoing.

The OCC is configuring and hardening its Microsoft 365 environment in alignment with secure baseline requirements issued under Binding Operational Directive 25-01, "Implementing Secure Practices for

Cloud Services." The OCC has also enhanced oversight of the contractor-led management of the Microsoft email environment.

As mentioned above, the OCC has partnered with Microsoft GHOST, as well as Mandiant and CrowdStrike, well known cybersecurity forensics firms, to perform a full investigation relating to the incident. Mandiant and CrowdStrike have both reviewed all activity within OCC's Microsoft Cloud tenant and verified there has been no indication of additional activity or lateral movement within OCC IT systems by the threat actor. On April 10, Mandiant further confirmed the breached account existed solely in the cloud environment, and their analysis found no evidence of compromise affecting other accounts in the tenant.

Technical information on the nature of the attack and indicators of compromise will be shared via U.S. Treasury in an OCCIP circular, on the Project Fortress Threat Feed platform and also through FS-ISAC.

Further, the OCC is expeditiously working to engage outside counsel to thoroughly evaluate the OCC's current IT security policies and procedures to improve its ability to prevent, detect, and remediate potential security incidents going forward. The OCC is committed to acting on recommendations made as a result of the evaluation.

The OCC and one of its contractors are currently working to review the content of all compromised email communications and attachments, including determining whether any of the compromised information has been found on the dark web. Information that was accessed includes financial supervision information provided by OCC supervised institutions and non-public OCC information. Efforts to determine if any bank customer information was compromised are ongoing.

What you can expect: The OCC is committed to ensuring its supervised institutions are informed of its efforts to address the breach and to fortify its information security systems. To this end, the OCC will host regular meetings with regulated banks, savings associations, and service providers to ensure open lines of communication and share current information about findings and the status of efforts underway to resolve the incident.

The OCC will inform each regulated institution if it determines the unauthorized user accessed information specific to that institution for their awareness. The OCC also will provide all supervised institutions with email user domains that were included in the compromised information so they may determine what information or data they may have sent to OCC users during the timeframe of the unauthorized access.

The OCC is engaging with industry Chief Information Security Officers (CISOs) to discuss industry best practices to further ensure the security of its systems.

In an abundance of caution, Mandiant is currently conducting a thorough review of both BankNet and the Large File Transfer (LFT) system which many regulated institutions use to share supervisory information. While OCC conducts regular penetration tests and security assessments on BankNet and other OCC communication systems, we have requested this additional comprehensive review to confirm

its security. The OCC will share information from Mandiant when this review has been completed. The OCC has requested CrowdStrike conduct a similar assessment and will also share their findings.

We recognize regulated institutions may have questions about their provision of requested supervisory information for OCC examinations. OCC examiners are available to work with individual institutions to answer their questions and ensure the secure exchange of required supervisory information.

The OCC is committed to the security of its information systems and will take every action necessary to ensure remediation of the deficiencies that contributed to this incident and to ensure full accountability for any organizational or structural deficiencies that contributed to this incident.

If you have any questions, please reach out to your EIC or portfolio manager.

Sincerely,

Rodney E. Hood
Acting Comptroller of the Currency
Office of the Comptroller of the Currency